UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/869,966	09/14/2001	Louis Guillou	9320.133USWO	4277

23552 7590 03/17/2006

MERCHANT & GOULD PC
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/869,966	GUILLOU ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *13-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *13,17 and 21* is/are rejected.

7)☒ Claim(s) *14-16,18-20 and 22-24* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 3/3/2006 was received and considered.

2. Claims 13-24 are pending.

Response

3. The response received indicates that claim 27 has been cancelled from the '918 application. However, upon the issuance of application number 10/089,662, an outstanding double patenting rejection is considered relevant. Additionally, applicant is notified of double patenting issues with applications 09/889,918, 10/089,646 & 10/471,884. Accordingly, the finality of the previous rejection is withdrawn and this action replaces the previous action as the final Office Action on the merits.

Double Patenting

4. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5. Claims 13, 17 & 21 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 19, 27, 28 & 29 of copending Application No. 10/089,662 in view of IBM Technical Disclosure Bulletin v36 n10

10-93 p413-416. The '662 application claims recite a processor and memory, wherein the processor performs a substantially equivalent key-obtaining steps except the '662 application fails to claim that the prime factors are congruent to 3 mod 4. However, IBM teaches that requiring that N be a Blum integer and hence that p and q (the prime factors) be congruent to 3 mod 4 makes the solution easier for the prover of an asymmetric authentication protocol (p. 413, ¶7). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine p_1 and p_2 such that $p_1 \equiv 3 \bmod 4$ and $p_2 \equiv 3 \bmod 4$. One of ordinary skill in the art would have been motivated to perform such a modification to make the proving step easier, as taught by IBM (p. 413, ¶7). This application 10/089,662 is not yet an issued U.S. Patent, however, the claims in question have been allowed. Therefore, when the '662 application issues, this rejection will be a non-provisional double patenting rejection.

6. Claims 13, 17 & 21 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 19 & 28 of copending Application No. 09/889,918 in view of IBM Technical Disclosure Bulletin v36 n10 10-93 p413-416. The '918 application claims recite a processor and memory, wherein the processor performs a substantially equivalent key-obtaining steps except the '918 application fails to claim that the prime factors are congruent to 3 mod 4. However, IBM teaches that requiring that N be a Blum integer and hence that p and q (the prime factors) be congruent to 3 mod 4 makes the solution easier for the prover of an asymmetric authentication protocol (p. 413, ¶7). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine p_1 and p_2 such that $p_1 \equiv 3 \bmod 4$ and $p_2 \equiv 3 \bmod 4$. One of ordinary skill

in the art would have been motivated to perform such a modification to make the proving step easier, as taught by IBM (p. 413, ¶7).

7. Claims 13, 17 & 21 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of copending Application No. 10/089,646 in view of IBM Technical Disclosure Bulletin v36 n10 10-93 p413-416. The '646 application claims recite a processor and memory, wherein the processor performs a substantially equivalent key-obtaining steps except the '646 application fails to claim that the prime factors are congruent to 3 mod 4. However, IBM teaches that requiring that N be a Blum integer and hence that p and q (the prime factors) be congruent to 3 mod 4 makes the solution easier for the prover of an asymmetric authentication protocol (p. 413, ¶7). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine p_1 and p_2 such that $p_1 \equiv 3 \bmod 4$ and $p_2 \equiv 3 \bmod 4$. One of ordinary skill in the art would have been motivated to perform such a modification to make the proving step easier, as taught by IBM (p. 413, ¶7).

8. Claims 13, 17 & 21 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 29 of copending Application No. 10/471,884 in view of IBM Technical Disclosure Bulletin v36 n10 10-93 p413-416. The '884 application claims recite a processor and memory, wherein the processor performs a substantially equivalent key-obtaining steps except the '884 application fails to claim that the prime factors are congruent to 3 mod 4. However, IBM teaches that requiring that N be a Blum integer and hence that p and q (the prime factors) be congruent to 3 mod 4 makes the solution easier for the prover of an asymmetric authentication protocol (p. 413, ¶7). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was made to determine p_1 and p_2 such that $p_1 \equiv 3 \bmod 4$ and $p_2 \equiv 3 \bmod 4$. One of ordinary skill in the art would have been motivated to perform such a modification to make the proving step easier, as taught by IBM (p. 413, ¶7).

This is a provisional obviousness-type double patenting rejection.

Allowable Subject Matter

9. Claims 13-24 contain allowable subject matter and would be allowed upon overcoming the provisional double patenting rejection.

10. Claims 14-16, 18-20 & 22-24 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

11. The following is an examiner's statement of reasons for allowance: Similarly to applicant's statement on p. 2 of the previous response, the prior art relied upon fails to teach or suggest determining a modulus equal to the product of at least two prime factors where the second factor is complementary to the first with respect to a chosen base number, calculating public values through $G_i \equiv g_i^{\,2} \bmod n$ and calculating private values by solving either the equation $G_i \cdot Q_i^{\,v} \equiv 1 \bmod n$ or $G_i \equiv Q_i^{\,v} \bmod n$ where the public exponent v is such that $v = 2^k$ in combination with the other elements of the claim. Menezes discloses choosing prime factors p and q and solving $ed = 1 \bmod (p-1)(q-1)$, but lacks computing multiple private values (§8.2.1). Further, Menezes discloses the prime factors being congruent to 3 mod 4 (§8.7.2). Okamoto teaches generating multiple public and private parameters (p. 36).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-8300
(for formal communications intended for entry)
Or:
(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS

March 13, 2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100